JOURNAL OF ALGEBRA **183,** 913–928 (1996)
ARTICLE NO. 0244

Cross-Sections for p-Adically Closed Fields

Philip Scowcroft*

Wesleyan University, Middletown, Connecticut 06459

Communicated by Leonard Lipshitz

INTRODUCTION

If F is a field with non-Archimedean valuation $v\colon F^* \twoheadrightarrow G$, a cross-section for the valued field (F, v) is a group homomorphism $\pi\colon G \to F^*$ that is a right inverse to v. So if p is prime and $v_p : \mathbf{Q}_p^* \twoheadrightarrow \mathbf{Z}$ is the p-adic valuation,

$$\pi(n) = p^n$$

is a cross-section for $(\mathbf{Q}_p, v_p)$. Another class of examples arises from fields of generalized power series [9, p. 23]: if F is any field, $(\Gamma, <)$ is any ordered Abelian group, and $F((t^\Gamma))$ is the field of power series $\sum_{\gamma \in \Gamma} a_\gamma t^\gamma$ with coefficients $a_\gamma \in F$ and support $\{\gamma \in \Gamma : a_\gamma \neq 0\}$ well-ordered by $<$, then $F((t^\Gamma))$ has valuation

$$\sum_{\gamma \in \Gamma} a_\gamma t^\gamma \neq 0 \mapsto \text{the least } \gamma \in \Gamma \text{ with } a_\gamma \neq 0$$

and cross-section $\gamma \in \Gamma \mapsto t^\gamma$.

If p is prime, a p-valued field [8, p. 7] is a valued field, of characteristic zero, in which p has minimal positive value and whose residue field has p elements. A p-valued field (F, v) is p-adically closed just in case no algebraic extension F' of F with valuation v' extending v is p-valued. The class of p-adically closed fields is to $(\mathbf{Q}_p, v_p)$ as the class of real-closed fields is to $\mathbf{R}$: see [8, Section 1] for a discussion of analogies between these classes of fields.

In their fundamental work on p-adically closed fields [1], Ax and Kochen found it convenient to work with p-adically closed fields having

* The research reported here was supported by NSF Grant DMS-9007990.

0021-8693/96 $18.00

cross-sections. Certain p-adically closed fields—those that are "ω-pseudo-complete" [1, p. 614]—always have cross-sections [1, p. 636], and in fact normalized ones: cross-sections that send the group element of least positive value to p. Cherlin [4, pp. 44–46] later showed that all $\aleph_1$-saturated p-adically closed fields have normalized cross-sections, but no further study of cross-sections was needed to develop the general theory of p-adically closed fields.

When studying semialgebraic equivalence relations over $\mathbf{Q}_p$, I grew interested in finding a p-adically closed field without a cross-section. Discovering none in the literature, I eventually built such a field, and found necessary and sufficient conditions for the existence of (normalized) cross-sections. These conditions appear, after the preliminary lemmas of Section 1, in Section 2, and are followed in Section 3 by a proof that any cross-section for $\mathbf{Q}_p$ extends to a cross-section for any p-adically closed extension of $\mathbf{Q}_p$. Section 4 then shows that if (F, v) is a p-adically closed field in which $(\mathbf{Q}_p, v_p)$ does not embed, then (F, v) has a p-adically closed extension without a cross-section. Section 5 refines this result by producing, among other examples, p-adically closed fields that have cross-sections but lack normalized ones. The proofs of these results will use model-theoretic techniques explained in [3].

I am grateful to A. Macintyre and A. Pillay for helpful suggestions at an early stage of my work.

1. SOME BACKGROUND INFORMATION

The Introduction singles out p-adically closed fields as maximal elements of a partially ordered class of p-valued fields. One may also characterize a p-adically closed field in terms referring only to the field itself [8, p. 34]. A valued field (F, v) is p-adically closed just in case it is p-valued and Henselian and its value group is a $\mathbf{Z}$-group; a $\mathbf{Z}$-group is an ordered Abelian group G, with least positive element 1, such that for each positive integer n G/nG has exactly n elements.

Some terminology from [8, 2.2] will prove useful in what follows. Let (F, v) be p-adically closed. If G is F's value group and 1 is the least positive element of G, one may identify the subgroup generated by 1 with $\mathbf{Z}$. It is a convex subgroup of G, whose quotient by $\mathbf{Z}$ becomes the value group of the coarse valuation

$$\dot{v}\colon F^* \xrightarrow{v} G \xrightarrow{q} G/\mathbf{Z}$$

of (F, v) (q is the usual quotient map). Since every rational number has coarse value zero, $(F, \dot{v})$'s residue field F°—the core field of F—has characteristic zero. If $R_{\dot{v}}$ is the valuation ring of $(F, \dot{v})$ and $x \in R_{\dot{v}} \mapsto x^\circ \in F^\circ$ is the residue map, one may define a valuation $\mathring{v}$: $(F^\circ)^* \to \mathbf{Z}$ of F° by the condition

$$\mathring{v}(x^\circ) = v(x).$$

Exploiting analogous properties of (F, v), one may show that $(F^\circ, \mathring{v})$ is p-valued and Henselian: so $(F^\circ, \mathring{v})$ is p-adically closed. Because $\mathring{v} \upharpoonright \mathbf{Q} = v_p \upharpoonright \mathbf{Q}$ and the residue field of F° is the field with p elements, any element of F° is the p-adic limit of a sequence of rational numbers: so one may embed $(F^\circ, \mathring{v})$ in $(\mathbf{Q}_p, v_p)$. Because any embedding of $(F^\circ, \mathring{v})$ in $(\mathbf{Q}_p, v_p)$ is the identity on $\mathbf{Q}$, $(\mathbf{F}^\circ, \mathring{v})$ is isomorphic to a unique valued subfield of $(\mathbf{Q}_p, v_p)$. One may therefore view $(F^\circ, \mathring{v})$ as a valued subfield of $(\mathbf{Q}_p, v_p)$. Yet since $(F, \dot{v})$ is Henselian of residue characteristic zero, one may exploit Zorn's lemma to find a field $\hat{F} \subseteq R_{\dot{v}}$ isomorphic to F° under $x \mapsto x^\circ$ [7, p. 406]. So as valued fields, $(\hat{F}, v)$ and $(F^\circ, \mathring{v})$ are isomorphic. (F, v) may contain many valued subfields $(\hat{F}, v)$ with this property, but since all are isomorphic to a unique valued subfield of $\mathbf{Q}_p$, arbitrary selection of a single such $(\hat{F}, v)$ allows one to view $(F^\circ, \mathring{v})$ as a valued subfield both of (F, v) and of $(\mathbf{Q}_p, v_p)$.

Finally, if (F, v) and (F', v') are p-adically closed fields and $g: F \to F'$ is an embedding of fields, then g includes an embedding $\hat{g}: G \to G'$ of value groups, relative to which g is an embedding of valued fields. This result holds for two reasons: if (F, v) is p-adically closed and $x, y \in F^*$, $v(x) \leq v(y)$ just in case $x^2 + py^2$ is a square in F (when $p \neq 2$; when $p = 2$, $x^3 + p^2y^3$ should be a cube in F) [2, p. 4]; and the theory of p-adically closed fields in the language of rings is model complete [8, p. 86].[1] One may therefore restrict attention to field embeddings, instead of valued-field embeddings, in the class of p-adically closed valued fields.

2. A CRITERION FOR CROSS-SECTIONS

Let (F, v) be p-adically closed. For each $m \geq 2$ let

$$P_m^F = \{x \in F^* : x \text{ is an } m\text{th power in } F\}$$

[1] Reference [8, p. 86] proves the model-completeness of the theory of p-adically closed fields in a language that extends the language of rings by a function symbol for division and a predicate symbol for the valuation ring. Since the formula $\varphi(x/y)$ is equivalent to the formula $(y = 0 \,\&\, \varphi(0)) \vee (y \neq 0 \,\&\, \exists z(\varphi(z) \,\&\, yz = x))$, one may eliminate all occurrences of $/$ at the cost of introducing new existentially quantified variables. Also, both the valuation ring and its complement may be defined by existential formulas in the language of rings. Thus the theory of p-adically closed fields in the language of rings is also model-complete.

and

$$\mathscr{P}^F = \bigcap_{m \geq 2} P_m^F;$$

the superscript “F” will be dropped when there is no danger of confusion. Each P_m^F is a subgroup of finite index in $(F^*, \cdot)$ [2, p. 5] and so $\mathscr{P}^F$ is a subgroup of $(F^*, \cdot)$. If $x \in \mathscr{P}^{\mathbf{Q}_p}$, then $v(x) \in \mathbf{Z}$ is divisible by every positive integer and so is zero; also, the image of x in any quotient ring $Q = \mathbf{Z}_p/p^n\mathbf{Z}_p$ must be a unit and a $|Q^*|$th power in Q’s group of units Q^*; thus x is 1 modulo p^n for all $n \geq 1$, and $\mathscr{P}^{\mathbf{Q}_p} = \{1\}$. In general,

LEMMA 1. *$(\mathscr{P}^F, \cdot)$ is a divisible subgroup of $(F^*, \cdot)$.*

Proof. Say $x \in \mathscr{P}$ and $m \geq 2$. If x is not divisible by m in $\mathscr{P}$, then none of x’s mth roots in F^* belongs to $\mathscr{P}$. If these mth roots are $y_1, \ldots, y_k$, then for each $l = 1, \ldots, k$ there is $n_l \geq 2$ such that $y_l \notin P_{n_l}$. So if $n = \prod_l n_l$, no $y_l \in P_n$. Yet since $x \in \mathscr{P}$, $x = z^{mn}$ for some $z \in F^*$, and $z^n \in P_n$ is one of the mth roots of x. This contradiction implies that $\mathscr{P}$ is divisible.

Let R be the valuation ring of (F, v) and $U = U^F$ be the group of units of R.

LEMMA 2. *If $e \in U$, then $v(e - e') > \mathbf{Z}$ for some $e' \in F^\circ$.*

Proof. By the identifications made in Section 1, F° is isomorphic via $x \mapsto x^\circ$ to the residue field of $(F, \dot{v})$. So if $e \in U$, $v(e) = 0$, $\dot{v}(e) = 0$, and $e^\circ = (e')^\circ$ for some $e' \in (F^\circ)^*$. Thus $\dot{v}(e - e') > 0$ and $v(e - e') > \mathbf{Z}$.

Note that $e' \in F^\circ \cap U$.

If $e \in U$, say that $x \in F^*$ is of e-sort just in case for each $m \geq 2$, x lies in the same coset of P_m as some power of pe. Let

$$S_e = S_e^F = \{x \in F^* : x \text{ is of } e\text{-sort}\}.$$

Since $\{(pe)^l : l \in \mathbf{Z}\}$ and the P_m are subgroups of $(F^*, \cdot)$, S_e is also a subgroup.

These definitions allow one to state

THEOREM 1. *(F, v) has a cross-section if and only if $F^* = S_e U$ for some $e \in U$; in this case, (F, v) has a cross-section sending 1 to pe.*

Proof. Assume that (F, v) has a cross-section π. Since $v\pi 1 = 1 = vp$, $\pi 1 = pe$ for some $e \in U$. If $x \in F^*$, then

$$x = (\pi v x)\frac{x}{\pi v x},$$

where $x/\pi vx \in U$ because $vx = v\pi vx$; so the proof will be complete if $\pi vx \in S_e$. When $m \in \mathbf{Z}$ and α, β belong to F's value group G, write

$$\alpha = \beta \qquad \text{mod } m$$

when

$$\alpha - \beta = m\gamma \qquad \text{for some } \gamma \in G.$$

If $m \geq 2$, then since G is a $\mathbf{Z}$-group there is an integer $l \in [0, m)$ such that

$$vx = l \qquad \text{mod } m$$

($l = l1$ in G). So there is $y \in F^*$ for which

$$vx = l + mvy = v(p^l y^m),$$

and

$$\pi vx = \pi v(p^l y^m) = (\pi vp)^l (\pi vy)^m = (pe)^l (\pi vy)^m.$$

Thus πvx and $(pe)^l$ belong to the same coset of P_m. Since $m \geq 2$ is arbitrary, $\pi vx \in S_e$ as desired.

Now assume that $F^* = S_e U$ for some $e \in U$. Let $U^\circ = U \cap F^\circ$ and $\hat{U} = \{x \in U : v(x-1) > \mathbf{Z}\}$. U° and $\hat{U}$ are subgroups of $(U, \cdot)$, and $U^\circ \cap \hat{U} = \{1\}$ since $U^\circ \subseteq F^\circ \subseteq \mathbf{Q}_p$. If $x \in U$, then Lemma 2 provides $x' \in U^\circ$ with $v(x - x') > \mathbf{Z}$: so $v((x/x') - 1) > \mathbf{Z}$, $x/x' \in \hat{U}$, and $x = x'(x/x') \in U^\circ \hat{U}$. Thus U is the internal direct product of U° and $\hat{U}$. By Hensel's lemma in (F, v), $\hat{U} \subseteq U \cap \mathscr{P}$. Conversely, if $x \in U \cap \mathscr{P}$, Lemma 2 provides $x' \in U^\circ$ with $v(x - x') > \mathbf{Z}$; so $v((x'/x) - 1) > \mathbf{Z}$, $x'/x \in \mathscr{P}$ by Hensel's lemma, $x' \in \mathscr{P}$ since $x \in \mathscr{P}$, and $x' = 1$ since $x' \in F^\circ \subseteq \mathbf{Q}_p$ and $\mathscr{P} \cap \mathbf{Q}_p \subseteq \mathscr{P}^{\mathbf{Q}_p} = \{1\}$. Thus $\hat{U} = U \cap \mathscr{P}$, and Lemma 1 implies that $(\hat{U}, \cdot)$ is divisible.

Zorn's lemma provides a subgroup T of S_e maximal with respect to the following property: $\{(pe)^l : l \in \mathbf{Z}\} \subseteq T$ and $T \cap \hat{U} = \{1\}$ (note that $\hat{U} = U \cap \mathscr{P} \subseteq S_e$). Suppose $x \in S_e - T\hat{U}$. Because T is a proper subgroup of the group $\langle T \cup \{x\} \rangle \subseteq S_e$ generated by $T \cup \{x\}$, $\langle T \cup \{x\} \rangle \cap \hat{U} \neq \{1\}$, and there are $t \in T$, $l \in \mathbf{Z} - \{0\}$, and $u \in \hat{U} - \{1\}$ for which

$$tx^l = u.$$

Since $\hat{U}$ is divisible, there is $u' \in \hat{U}$ with $(u')^l = u$, and so $tx^l = (u')^l$ and

$$t = (x^{-1}u')^l = w^l$$

where $w = x^{-1}u' \in S_e$. If $w \in T\hat{U}$, a subgroup of S_e, then $x = w^{-1}u' \in (T\hat{U})\hat{U} = T\hat{U}$: so $w \notin T\hat{U}$, and as above there are $t' \in T$, $m \in \mathbf{Z}$, and

$u'' \in \hat{U} - \{1\}$ for which

$$t' w^m = u''.$$

Thus $(t')^l (w^l)^m = (u'')^l$ and $(t')^l t^m = (u'')^l$. Since $t, t' \in T$, $u'' \in \hat{U}$, and $T \cap \hat{U} = \{1\}$, $(u'')^l = 1$. Because $(F^\circ, v) \subseteq (F, v)$ are p-adically closed, F° is algebraically closed in F, and $u'' \in F^\circ$: so $u'' \in \hat{U} \cap F^\circ = \{1\}$, contrary to the choice of u''. This contradiction implies that $S_e = T\hat{U}$ is the internal direct product of T and $\hat{U}$.

By hypothesis, therefore,

$$F^* = (T\hat{U})U = (T\hat{U})(\hat{U}U^\circ) = T\hat{U}U^\circ.$$

In fact, F^* is the internal direct product of T, $\hat{U}$, and U°. Suppose that $t \in T$, $u_1 \in \hat{U}$, $u_2 \in U^\circ$, and $tu_1u_2 = 1$. Because $t = (u_1u_2)^{-1} \in U$, $t \in \mathscr{P}$: for if $t \notin P_m$ for some $m \geq 2$, then since $t \in S_e$, $t/(pe)^l \in P_m$ for some $l \in \mathbf{Z}$, m does not divide l in $\mathbf{Z}$—otherwise, $t \in P_m$—and $v(t) = l \bmod m$, contrary to the fact that $v(t) = 0$. Thus $t \in T \cap U \cap \mathscr{P} = T \cap \hat{U} = \{1\}$, $u_1u_2 = 1$ in the direct product $U^\circ \hat{U}$, and $u_1 = u_2 = 1$.

So for each $x \in F^*$ there is a unique $t \in T$ with $v(x) = v(t)$. Clearly, then, there is a map $\pi : G \to F^*$ sending any $v(x)$ to the unique $t \in T$ with $v(x) = v(t)$. Since v is a homomorphism and $pe \in T$ has value 1, one may easily check that π is a cross-section for (F, v) that sends 1 to pe.

Note that if e, $e' \in U$ and $v(e - e') > \mathbf{Z}$, then $S_e = S_{e'}$: for since $v((e/e') - 1) > \mathbf{Z}$, Hensel's lemma implies that $e/e' \in \mathscr{P}$, and so $(pe)^l/(pe')^l \in \mathscr{P}$ for every $l \in \mathbf{Z}$ and $(pe)^l$, $(pe')^l$ always lie in the same coset of any P_m. Lemma 2 and Theorem 1 thus combine to show that if (F, v) has a cross-section, it has a cross-section sending 1 to pe for some $e \in F^\circ$. The restriction of this cross-section to $\mathbf{Z}$ gives a cross-section for (F°, v); so one may study the cross-sections for (F, v) by asking which cross-sections for (F°, v) extend to cross-sections for (F, v).

3. p-ADICALLY CLOSED FIELDS CONTAINING $\mathbf{Q}_p$

This section is devoted to a proof of

THEOREM 2. *If (M, v_M) is a p-adically closed field in which $\mathbf{Q}_p$ is embedded, then any cross-section for $(\mathbf{Q}_p, v_p)$ extends to a cross-section for (M, v_M).*

Ax and Kochen prove that any ω-pseudo-complete p-adically closed field has a normalized cross-section [1, p. 636], but they invoke ω-pseudo-completeness only to embed $\mathbf{Q}_p$ in the field under consideration. So much of the present result is implicit in their work, though the proof here proceeds along different lines.

Proof. Remarks at the end of Section 1 allow one to regard $(\mathbf{Q}_p, v_p)$ as a valued subfield of (M, v_M). Each $P_m^{\mathbf{Q}_p}$ is an open subgroup of $\mathbf{Q}_p^*$ of finite index, and one may choose coset representatives from $\mathbf{Z}$ [2, p. 5]. So for each $m \geq 2$, let the $a_{m,i}$ be finitely many integers, with $v_p(a_{m,i}) \in [0, m)$, that represent the distinct cosets of $P_m^{\mathbf{Q}_p}$ in $\mathbf{Q}_p^*$. The model-completeness result mentioned in Section 1 implies that for any p-adically closed K, the $a_{m,i}$ serve as coset representatives for P_m^K in K^*.

Let π be any cross-section for $\mathbf{Q}_p$. $\pi(1) = pe$ for some $e \in U^{\mathbf{Q}_p}$. If $M^* \subseteq S_e^M U^M$, then Theorem 1 implies that M has a cross-section sending 1 to pe, and this cross-section certainly extends π.

So, suppose $x \in M^*$. For each $n \geq 2$ let k_n be the unique integer in $[0, n)$ with

$$v_M(x) = k_n \qquad \bmod n$$

and $b_n = a_{n,i}$ represent the coset of P_n^M determined by $x/(pe)^{k_n}$. Since n divides $v_M(x/(pe)^{k_n})$ in $v_M(M^*)$ and $v_M(b_n) \in [0, n)$, $v_M(b_n) = 0$ for all $n \geq 2$. Clearly

$$\frac{x}{(pe)^{k_{n!}}} \in b_{n!} P_{n!}^M \subseteq \bigcap_{2 \leq m \leq n} b_m P_m^M$$

for each $n \geq 2$, and so the sentence

$$\exists y \neq 0 \Big(v(y) = 0 \bmod n! \,\&\, \bigwedge_{2 \leq m \leq n} \exists z (b_m z^m = y) \Big) \tag{1}$$

is true in (M, v_M). Because $(\mathbf{Q}_p, v_p) \subseteq (M, v_M)$ and $Th(\mathbf{Q}_p, v_p) = Th(M, v_M)$ is model-complete,[2] $(\mathbf{Q}_p, v_p) \preceq (M, v_M)$ and each sentence (1) is true in $(\mathbf{Q}_p, v_p)$. Thus each sentence

$$\exists s \neq 0 \Big(v(s) = 0 \qquad \& \qquad \bigwedge_{2 \leq m \leq n} \exists z (b_m z^m = s) \Big) \tag{2}$$

is true in $(\mathbf{Q}_p, v_p)$: for if $y \in \mathbf{Q}_p$ satisfies the body of (1), $s = p^{-v_p(y)} y$ satisfies the body of (2). So for each $n \geq 2$,

$$U^{\mathbf{Q}_p} \cap \bigcap_{2 \leq m \leq n} b_m P_m^{\mathbf{Q}_p} \neq \emptyset.$$

Because $(U^{\mathbf{Q}_p}, \cdot\,)$ is a compact group and each $U^{\mathbf{Q}_p} \cap b_m P_m^{\mathbf{Q}_p}$ is a clopen subset of $U^{\mathbf{Q}_p}$,

$$U^{\mathbf{Q}_p} \cap \bigcap_{2 \leq n} b_n P_n^{\mathbf{Q}_p} \neq \emptyset.$$

[2] Model-completeness of the theory of p-adically closed fields in a two-sorted language appropriate to (M, v_M) follows from the model-completeness results already quoted, since both M's value group and v_M are interpretable in the ring M.

If u is an element of this set, then since $\mathbf{Q}_p \subseteq M$, $u \in U^M$ and

$$\frac{x/(pe)^{k_n}}{u} \in P_n^M$$

for each $n \geq 2$. So for each $n \geq 2$, x/u is in the same coset of P_n^M as $(pe)^{k_n}$, $x/u \in S_e^M$, and $x \in S_e^M U^M$ as desired.

4. FIELDS WITHOUT CROSS-SECTIONS

The next two sections will show that Theorem 2 does not extend to p-adically closed fields in which $\mathbf{Q}_p$ does not embed. Starting with a p-adically closed (F, v), both sections will find a p-adically closed (K, w) that contains both (F, v) and a special $a \in K^*$ infinitesimal with respect to F: i.e., $w(a) > w(x) = v(x)$ for all $x \in F^*$. Attention will then shift to L, the smallest p-adically closed subfield of K that contains $F(a)$. Because the theory of p-adically closed fields in the language of rings admits definable Skolem functions [5, p. 627], L will be the definable closure—here, the algebraic closure—of $F(a)$ in K.

A special description of L's elements will prove useful in what follows. For each $n \geq 2$ there is a formula in the language of rings that defines, over any p-adically closed field, a continuous nth root function on the set of nth powers; in what follows $\sqrt[n]{x}$ will be the value of this function at the nth power x. With the help of this notation one may state

LEMMA 3. *Let $(F, v) \subseteq (K, w)$ be p-adically closed fields. If $a \in K^*$ is infinitesimal with respect to F and $L \subseteq K$ is the algebraic closure of $F(a)$ in K, then $(L, w \upharpoonright L)$ is p-adically closed, and for every $g \in L$ there are $c \in F$, $u \in L$, and integers $n \geq 2$ and m for which*

$$g = c\left(\sqrt[n]{a/a_{n,i}}\right)^m u,$$

where $a \in a_{n,i} P_n^K$ and $w(u-1) > v(F^*)$.

The result follows immediately from Theorem 1 of [10] and well-known results in the model theory of p-adically closed fields; the proof will not be given here.

Now for the proof of

THEOREM 3. *If (F, v) is a p-adically closed field in which $\mathbf{Q}_p$ does not embed, then (F, v) has a p-adically closed extension without a cross-section.*

Proof. Assume that $\mathbf{Q}_p$ does not embed in the p-adically closed field F. Since F's core field $F^\circ \subseteq F$ is a subfield of $\mathbf{Q}_p$, F° must be a proper subfield of $\mathbf{Q}_p$. $\mathbf{Q}_p$ is the only subfield of $\mathbf{Q}_p$ that contains every p-adic number of value zero: so there is $a \in \mathbf{Q}_p - F^\circ$ of value zero. For each $m \geq 2$ let $b_m = a_{m,i}$ represent the coset of $P_m^{\mathbf{Q}_p}$ to which a belongs, and let

$$\Sigma = \{\exists z \neq 0(b_m z^m = y) : m \geq 2\} \cup \{v(y) > v(b) : b \in F^*\},$$

a set of formulas in the language of $(F, v)_F$. Any finite subset of Σ may be satisfied in $(F, v)_F$: for if $n \geq 2$ is arbitrary and $b \in F^*$ has positive value, then

$$b_{n!}b^{n!} \in \bigcap_{2 \leq m \leq n} b_m P_m^F$$

and

$$v\left(b_{n!}b^{n!}\right) = v(b^{n!}) > v(b);$$

note that every $v_p(b_k) = 0$ since $a \in b_k P_k^{\mathbf{Q}_p}$, $v_p(a) = 0$, and $v_p(b_k) \in [0, k)$. The compactness theorem therefore provides a p-adically closed extension (K, w) of (F, v) in which some $b \in K$ satisfies every formula of Σ. Lemma 3, and the model-completeness of $Th(F, v) = Th(K, w)$, allow one to assume that K is the algebraic closure of $F(b)$ in K; so Lemma 3 also describes all the elements of K.

Because $b \in \bigcap_m b_m P_m^K$ and each $w(b_m) = 0$, $w(b)$ is divisible by every positive integer. So if (K, w) has a cross-section π, $\pi w(b) \in \mathscr{P}^K$ because π is a homomorphism. One may therefore show that (K, w) lacks a cross-section by showing that no $g \in K$ with the same value as b belongs to $\mathscr{P}^K$.

Assume, to the contrary, that $g \in \mathscr{P}^K$ has the same value as b. Lemma 3 implies that there are $c \in F$, $u \in K$, and integers $n \geq 2$ and m for which $w(u-1) > w(F^*)$ and

$$g = c\left(\sqrt[n]{b/b_n}\right)^m u.$$

So

$$\begin{aligned} w(b) = w(g) &= w\left(c\left(\sqrt[n]{b/b_n}\right)^m u\right) \\ &= w(c) + \frac{m}{n} w(b). \end{aligned}$$

Because $w(b) > w(F^*)$ and $c \in F^*$, $m/n = 1$ and

$$g = cbb_n^{-1}u.$$

Since $w(u-1)$ is greater than any integer, Hensel's lemma places u in $\mathscr{P}^K$, a subgroup of $(K^*, \cdot)$: so $cbb_n^{-1} \in \mathscr{P}^K$ and b and $c^{-1}b_n$ belong to the same coset of every P_m^K. Because $w(g) = w(b)$, $w(c^{-1}b_n) = 0$. Lemma 2 thus provides $d \in F^\circ$ with $w(c^{-1}b_n - d) > \mathbf{Z}$. Hensel's lemma again implies that $c^{-1}b_n$ and d belong to the same coset of every P_m^K, and so b and d belong to the same coset of every P_m^K. Since b satisfies Σ, $d \in \bigcap_m b_m P_m^K$, and so

$$d \in \bigcap_{m \geq 2} b_m P_m^{F^\circ}$$

because $F^\circ \subseteq K$ is p-adically closed. Thus

$$d \in \bigcap_{m \geq 2} b_m P_m^{\mathbf{Q}_p}.$$

Since $\mathscr{P}^{\mathbf{Q}_p} = \{1\}$ and $a \in \bigcap_m b_m P_m^{\mathbf{Q}_p}$, $a = d \in F^\circ$, contrary to the choice of a. This contradiction implies that no $g \in \mathscr{P}^K$ has the same value as b and completes the proof of Theorem 3.

5. FIELDS WITHOUT NORMALIZED CROSS-SECTIONS

If (F, v) is p-adically closed, so is $(F^\circ, v \upharpoonright F^\circ) \subseteq (F, v)$. Since $F^\circ \subseteq \mathbf{Q}_p$, the cross-sections for $(F^\circ, v \upharpoonright F^\circ)$ are in one-to-one correspondence $\pi \mapsto \pi(1)$ with F°'s elements of value one. When $F^\circ = \mathbf{Q}_p$, Section 3 shows that every cross-section for $(F^\circ, v \upharpoonright F^\circ)$ extends to a cross-section for (F, v); when $F^\circ \subset \mathbf{Q}_p$, Section 4 shows that no cross-section for $(F^\circ, v \upharpoonright F^\circ)$ need extend to a cross-section for (F, v). By exploiting more detailed information about $\mathbf{Q}_p$'s multiplicative group, the present section will show that other cases may also occur: for example, there are p-adically closed fields, with cross-sections, that lack normalized cross-sections.

In the ring $\mathbf{Z}_p$ of p-adic integers let θ be a primitive $(p-1)$th root of unity (or -1, if $p = 2$), G be the cyclic subgroup of $(\mathbf{Q}_p^*, \cdot)$ generated by θ, and

$$e = \begin{cases} 1 + p & \text{if } p \neq 2 \\ 1 + p^2 & \text{if } p = 2. \end{cases}$$

According to [6, p. 246], $(Q_p^*, \cdot)$ is isomorphic to the direct product of $(\mathbf{Z}, +)$, G, and $(\mathbf{Z}_p, +)$; the mapping

$$(m, \gamma, a) \mapsto p^m \gamma e^a$$

is an isomorphism of $\mathbf{Z} \times G \times \mathbf{Z}_p$ onto $\mathbf{Q}_p^*$. Because the only elements of $\mathbf{Z} \times G \times \mathbf{Z}_p$ divisible by p^m for all $m \geq 1$ are the elements of $\{0\} \times G \times \{0\} - \{(0,1,0)\}$, if $p = 2$ one may conclude that

LEMMA 4. $\bigcap_{m \geq 1} P_{p^m}^{\mathbf{Q}_p} = G$ (*or* $\{1\}$, *if* $p = 2$).

Note also that since $\mathbf{N}$ is dense in $\mathbf{Z}_p$, $\{p^m \gamma e^a : m \in \mathbf{Z},\ \gamma \in G,$ and $a \in \mathbf{N}\}$ is dense in $\mathbf{Q}_p^*$. Because the cosets of each $P_n^{\mathbf{Q}_p}$ are open in $\mathbf{Q}_p^*$, one may choose representatives for the cosets of $P_n^{\mathbf{Q}_p}$ from $\{p^m \gamma e^a : m \in [0, n),\ \gamma \in G,$ and $a \in \mathbf{N}\}$. Since the elements of this set are algebraic p-adic numbers, they belong to every p-adically closed field and can serve as representatives for the cosets of P_n^F in any p-adically closed F. The proof of Lemma 3, which mentions coset representatives $a_{n,i}$ of P_n, works for any representatives that are algebraic p-adic numbers with values in $[0,n)$; so one may assume that the $a_{n,i}$'s belong to $\{p^m \gamma e^a : m \in [0, n),$ $\gamma \in G,$ and $a \in \mathbf{N}\}$.

One may now state

THEOREM 4. *Let (F, v) be a p-adically closed field, in which $\mathbf{Q}_p$ does not embed, which has both a normalized cross-section and a cross-section sending* 1 *to pe. There are p-adically closed extensions (K, v_K) and (L, v_L) of (F, v) such that (K, v_K) has a cross-section sending* 1 *to pe, but no normalized cross-section, while (L, v_L) has a normalized cross-section, but no cross-section sending* 1 *to pe.*

Proof. Because similar arguments produce (K, v_K) and (L, v_L), only (K, v_K) will be studied in detail.

Let (F, v) be as described. As in the proof of Theorem 3, one knows that F° is a proper subfield of $\mathbf{Q}_p$. Let

$$S = \begin{cases} 1 + p\mathbf{Z}_p & \text{if } p \neq 2 \\ 1 + p^2\mathbf{Z}_p & \text{if } p = 2. \end{cases}$$

Since $\mathbf{Q}_p$ is the smallest subfield of $\mathbf{Q}_p$ that contains S, there is an element $a \in S - F^\circ$. By [6, p. 246] there is a sequence $\{k_n\}_{n=1}^\infty$ of natural numbers for which

$$a = \lim_{n \to \infty} e^{k_n}$$

in $\mathbf{Q}_p$. Since $\mathscr{P}^{\mathbf{Q}_p} = \{1\}$ and each $P_n^{\mathbf{Q}_p}$ is an open subset of $\mathbf{Q}_p$, one may suppose that

$$a/e^{k_n} \in P_{p^n}^{\mathbf{Q}_p} \qquad \text{for each } n \geq 1. \tag{1}$$

If $l_n \in [0, p^n)$ is congruent to k_n modulo p^n for each $n \geq 1$, then (1) also holds with k_n replaced by l_n.

Let

$$\Sigma_1 = \{\alpha = k_n \bmod p^n : n \geq 1\} \cup \{\alpha > v(f) : f \in F^* \text{ and } v(f) > 0\},$$

a set of formulas, in the language of ordered Abelian groups, with parameters from $v(F^*)$. Let π be a cross-section for (F, v) with $\pi(1) = pe$. One may show that Σ_1 is consistent with $Th(F, v, \pi)_F$ by showing that every finite subset

$$\Sigma_1' = \{\alpha = k_1 \bmod p, \ldots, \alpha = k_c \bmod p^c\} \cup \{\alpha > v(f)\}$$

is satisfied in $(F, v, \pi)_F$. Each a/e^{k_n} is a p^nth power, and $p^m \mid p^n$ if $1 \leq m \leq n$: so $e^{k_c - k_d}$ is a p^dth power whenever $1 \leq d \leq c$. Applying the inverse of the isomorphism described at the start of this section, one concludes that p^d divides $k_c - k_d$ in $\mathbf{Z}_p$ when $1 \leq d \leq c$. Since p^d is a power of p and $k_c - k_d$ is an integer, p^d divides $k_c - k_d$ in $\mathbf{Z}$ when $1 \leq d \leq c$. Thus $k_c + p^c v(f) \in v(F^*)$ satisfies Σ_1': when $1 \leq d \leq c$, $k_c + p^c v(f) = k_c = k_d \bmod p^d$, and since $v(f) > 0$ and $k_c \geq 0$, $k_c + p^c v(f) \geq p^c v(f) > v(f)$.

The completeness theorem provides a p-adically closed field $(M, v_M, \pi_M) \succeq (F, v, \pi)$ and an element $\beta \in v(M^*)$ that satisfies Σ_1. If $b = \pi_M \beta$, then $v_M(b) = v_M \pi_M \beta = \beta > v(f)$ for all $f \in F^*$ and

$$b \in (pe)^{k_n} P_{p^n}^M \qquad \text{for all } n \geq 1$$

because $\pi_M : v(M^*) \to M^*$ is a homomorphism sending 1 to pe. For each $n \geq 2$ let $b_n = a_{n,i}$ represent the coset of P_n^M to which b belongs. If $n \geq 2$, $b_n = p^m \gamma e^k$ for some $\gamma \in G$ and integers $m \in [0, n)$ and k, and there is $w \in M$ for which $b_n w^n = b$. So

$$(\pi_M v_M w)^n = \frac{\pi_M v_M b}{\pi_M v_M b_n} = \frac{\pi_M v_M \pi_M \beta}{(\pi_M v_M p)^m (\pi_M v_M \gamma)(\pi_M v_M e)^k}$$

$$= \frac{b}{(pe)^m}$$

since $e, \gamma \in \mathbf{Z}_p$ are units and π_M is a cross-section for (M, v) that sends $1 = vp$ to pe. One may therefore write

$$(\pi_M v_M w)^n = \frac{b}{p^m \gamma e^k} \gamma e^{k-m} = \frac{b}{b_n} \gamma e^{k-m}$$

$$= \sqrt[n]{b/b_n}^{\,n} \gamma e^{k-m},$$

and there is an algebraic unit $\gamma_n \in \mathbf{Z}_p$ for which

$$\sqrt[n]{b/b_n}\, \gamma_n = \pi_M v_M w.$$

As in the proof of Theorem 1, $\pi_M v_M w$ is of e-sort: so for each $q \geq 2$ there is an integer $d_{n,q} \in [0, q)$ for which

$$\sqrt[n]{b/b_n}\,\gamma_n \in (pe)^{d_{n,q}} P_q^M.$$

Of course, $b = \pi_M \beta$ is also of e-sort, and so for each $q \geq 2$

$$b \in (pe)^{d_q} P_q^M$$

for some integer $d_q \in [0, q)$; note that $d_{p^n} = l_n$ for each $n \geq 1$. One concludes that b satisfies

$$\begin{aligned} \Sigma = &\left\{\exists z \neq 0\left((pe)^{d_q} z^q = y\right) : q \geq 2\right\} \\ &\cup \{v(y) > v(f) : f \in F^* \text{ and } v(f) > 0\} \\ &\cup \left\{\exists z \neq 0\left((pe)^{d_{n,q}} z^q = \sqrt[n]{y/b_n}\,\gamma_n\right) : n, q \geq 2\right\} \end{aligned}$$

in M.

Let K be the algebraic closure of $F(b)$ in M and $v_K = v_M \restriction K$. (K, v_K) is a p-adically closed extension of (F, v), and by model-completeness b still satisfies Σ in (K, v_K) (note that the parameters in Σ are either algebraic p-adic numbers, and so in F, or belong to $v(F^*)$). To show that (K, v_K) has a cross-section sending 1 to pe, one may invoke Theorem 1 and show that $K^* = S_e U$. If $x \in K^*$, Lemma 3 says that

$$x = c\left(\sqrt[n]{b/b_n}\right)^m u,$$

where $c \in F^*$, $n \geq 2$ and m are integers, $u \in K$, and $v_K(u - 1) > v(F^*)$. Because b satisfies Σ, $\sqrt[n]{b/b_n}\,\gamma_n \in S_e$. Since γ_n is an algebraic unit, $\gamma_n \in U$, $\sqrt[n]{b/b_n} \in S_e U$, and $\sqrt[n]{b/b_n}^{\,m} u \in S_e U$. By hypothesis, $c \in F^* = S_e^F U^F \subseteq S_e U$: so $x \in S_e U$ as desired.

But (K, v_K) does not have a normalized cross-section. Otherwise, Theorem 1 implies that $b = gu$ for some $g \in S_1$ and $u \in U$, and by Lemma 3

$$g = c\left(\sqrt[n]{b/b_n}\right)^m u'$$

for some $c \in F^*$, integers $n \geq 2$ and m, and $u' \in K$ with $v_K(u' - 1) > v(F^*)$. Because $u \in U$,

$$\begin{aligned} v_K(b) = v_K(g) &= v_K(c) + \frac{m}{n}\left(v_K(b) - v_K(b_n)\right) \\ &= v(c) + \frac{m}{n}\left(v_K(b) - v(b_n)\right); \end{aligned}$$

so since $v_K(b) > v(F^*)$, $m/n = 1$ and

$$g = cbb_n^{-1}u',$$

where $cb_n^{-1}u' \in U$. By hypothesis, there are integers $s_q \in [0, q)$ such that

$$g \in p^{s_q}P_q^K \qquad \text{for all } q \geq 2.$$

Since $b \in (pe)^{d_q}P_q^K$ for all $q \geq 2$, each

$$\left(cbb_n^{-1}u'/p^{s_q}\right)\left(b/(pe)^{d_q}\right)^{-1} \in P_q^K,$$

and so each $cb_n^{-1}u'e^{d_q}p^{d_q - s_q} \in P_q^K$. Now, $|d_q - s_q| \in [0, q)$, and $cb_n^{-1}u'e^{d_q} \in U$: so $d_q - s_q = 0$ for all $q \geq 2$, and

$$u = b/g = \left(b(pe)^{-d_q}/(gp^{-s_q})\right)e^{d_q} \in e^{d_q}P_q^K$$

for all $q \geq 2$. Since u is a unit, Lemma 3 implies that $u = c'u''$ for some $c' \in U^F$ and $u'' \in K$ with $v_K(u'' - 1) > v(F^*)$. So $u'' \in \mathscr{P}^k$ by Hensel's lemma, $c' \in e^{d_q}P_q^K$ for all $q \geq 2$, and

$$c' \in e^{d_q}P_q^F$$

since $c', e \in F$ and $(F, v) \preceq (K, v_K)$. Lemma 2 provides $h \in F^\circ \cap U$ with $v_K(c' - h) > \mathbf{Z}$: so

$$h \in e^{d_q}P_q^K \qquad \text{for all } q \geq 2$$

by Hensel's lemma. Letting $q = p^n$, one finds that

$$h \in e^{l_n}P_{p^n}^K \qquad \text{for all } n \geq 1$$

since $l_n = d_{p^n}$. Because a, $h \in \mathbf{Q}_p$ and

$$a \in e^{l_n}P_{p^n}^{\mathbf{Q}_p} \qquad \text{for all } n \geq 1,$$

one may conclude that

$$ah^{-1} \in \bigcap_{n \geq 1} P_{p^n}^{\mathbf{Q}_p} \subseteq G$$

by Lemma 4. Now, G is contained in any p-adically closed field: so $a \in hG \subseteq F^\circ$, contrary to the choice of a. Thus (K, v_K) lacks a normalized cross-section.

To build the p-adically closed extension (L, v_L) of (F, v) that has a normalized cross-section but lacks a cross-section sending 1 to pe, one makes just a few changes in the previous argument. So, π is now a normalized cross-section for (F, v). Thus $b \in p^{k_n} P^M_{p_n}$ for all $n \geq 2$ and $(\pi_M v_M w)^n = b/p^m$ in the first computations concerning $b = \pi_M \beta$. Also,

$$\sqrt[n]{b/b_n}\,\gamma_n \in p^{d_{n,q}} P^M_q$$

and

$$b \in p^{d_q} P^M_q$$

for each $q \geq 2$; so in the definition of Σ, each "pe" should be replaced by "p". If L is the algebraic closure of $F(b)$ in M and $v_L = v_M \restriction L^*$, one argues, as before, that (L, v_L) has a cross-section, but now it is normalized. Yet (L, v_L) has no cross-section taking 1 to pe because there are no $g \in S^L_e$ and $u \in U^L$ for which $b = gu$. For if such g, u exist, and $g \in (pe)^{s_q} P^L_q$ for all $q \geq 2$, then one may repeat the computation of b/g —with "p" and "pe" interchanged, and e^{d_q} replaced by its inverse—to conclude that $u^{-1} \in e^{d_q} P^L_q$ for all $q \geq 2$. So if $h \in F^\circ$ and $v(u^{-1} - h) > \mathbf{Z}$, one obtains a contradiction as before.

Note that one may assume that the cross-sections for (K, v_K) and (L, v_L) mentioned in Theorem 4 extend the relevant cross-sections for (F, v). If, for example, π is a normalized cross-section for (F, v), let $T \subseteq S^L_1$ be a subgroup maximal among those that contain $\operatorname{ran}(\pi)$ and intersect $\hat{U}^L$ trivially, and argue as in the proof of Theorem 1 to obtain a cross-section for (L, v_L) whose range is T; this cross-section will be normalized and extend π.

A QUESTION

Is there an informative classification of the cross-sections a p-adically closed field may have? A simple attempt at such a classification associates, with any p-adically closed (F, v), the set $C(F)$ of all $a \in F^\circ$ such that some cross-section for (F, v) sends 1 to pa. By Section 2, (F, v) has a cross-section if and only if $C(F) \neq \varnothing$. The results of Sections 3, 4 show that if $\mathbf{Q}_p$ embeds in F, then $C(F) = F^\circ \cap \mathbf{Z}^*_p = \mathbf{Z}^*_p$, while if $\mathbf{Q}_p$ does not embed in F, then $C(K) = \varnothing$ for some p-adically closed $K \supseteq F$. Section 5 shows that a nonempty $C(F)$ need not be a subgroup of $\mathbf{Z}^*_p$—since 1 need not belong to $C(F)$—and that the class of all $C(F)$ is only partially ordered by inclusion. One can show that a nonempty $C(F)$ is a subgroup of $\mathbf{Z}^*_p$ just in case $C(F)$ is closed under multiplication, but one might also wonder whether $C(F)$ is a subgroup just if it contains 1. And unless those $C(F)$'s that are not groups have some other interesting structure, one may also want to find a new object that better describes the cross-sections of (F, v).

REFERENCES

1. J. Ax and S. Kochen, Diophantine problems over local fields, I, II, *Am. J. Math* **87** (1965), 605–630, 631–648.
2. L. Bélair, Substructures and uniform elimination for p-adic fields, *Ann. Pure Appl. Logic* **39** (1988), 1–17.
3. C. C. Chang and H. J. Keisler, ''Model Theory,'' North-Holland, Amsterdam, 1990.
4. G. Cherlin, ''Model Theoretic Algebra: Selected Topics,'' Springer-Verlag, Berlin, 1976.
5. L. van den Dries, Algebraic theories with definable Skolem functions, *J. Symbolic Logic* **49** (1984), 625–629.
6. H. Hasse, ''Number Theory,'' Springer-Verlag, Berlin, 1980.
7. S. Kochen, The model theory of local fields, in ''Lecture Notes in Math.'' Vol. 499, Springer-Verlag, Berlin, 1975.
8. A. Prestel and P. Roquette, ''Formally p-Adic Fields,'' Springer-Verlag, Berlin, 1984.
9. O. F. G. Schilling, ''The Theory of Valuations,'' American Mathematical Society, New York, 1950.
10. P. Scowcroft, More on imaginaries in p-adic fields, *J. Symbolic Logic*, to appear.